Secrecy Performance of Wirelessly Powered Wiretap Channels

Secrecy Performance of Wirelessly Powered Wiretap Channels

Xin Jiang, *Student Member, IEEE,* Caijun Zhong, *Senior Member, IEEE,* Xiaoming Chen, *Senior Member, IEEE,* Trung Q. Duong, *Senior Member, IEEE,* Theodoros Tsiftsis, *Senior Member, IEEE,* and Zhaoyang Zhang, *Member, IEEE*

***Abstract*—This paper considers a wirelessly powered wiretap channel, where an energy constrained multi-antenna information source, powered by a dedicated power beacon, communicates with a legitimate user in the presence of a passive eavesdropper. Based on a simple time-switching protocol where power transfer and information transmission are separated in time, we investigate two popular multi-antenna transmission schemes at the information source, namely maximum ratio transmission (MRT) and transmit antenna selection (TAS). Closed-form expressions are derived for the achievable secrecy outage probability and average secrecy rate for both schemes. In addition, simple approximations are obtained at the high signal-to-noise ratio (SNR) regime. Our results demonstrate that by exploiting the full knowledge of channel state information (CSI), we can achieve a better secrecy performance, e.g., with full CSI of the main channel, the system can achieve substantial secrecy diversity gain. On the other hand, without the CSI of the main channel, no diversity gain can be attained. Moreover, we show that the additional level of randomness induced by wireless power transfer does not affect the secrecy performance in the high SNR regime. Finally, our theoretical claims are validated by the numerical results.**

***Index Terms*—Physical layer security, wireless power transfer, secrecy outage probability, average secrecy rate.**

I. Introduction

Recently, the rapidly increasing demands for high data rate wireless services have put a tremendous pressure on the energy consumption of battery-powered mobile devices. Hence, how to prolong the lifetime of these energy-constrained mobile devices has become a critical problem to be addressed. Responding to this, energy harvesting techniques, which scavenge energy from ambient environment such as wind and solar have been proposed as a promising solution. Nevertheless, harvesting energy from nature resources depends heavily on the locations and weather conditions, which fails to generate stable energy output, hence may not be suitable to power wireless devices with strict quality of service requirements. As a result, a new energy harvesting paradigm, generally referred to as wireless power transfer (WPT), has gained considerable attentions. By exploiting the radio frequency (RF) signals as a means for energy transportation, WPT enables reliable and stable energy supplies to mobile devices. Since RF signals are widely used as a medium for information transmission, incorporating the feature of WPT into wireless communications networks has emerged as a hot topic, generally referred to as simultaneously wireless information and power transfer (SWIPT) systems, and significant research effects have been devoted to understand the fundamental performance limitation as well as design efficient SWIPT systems, see for instances [1]–[9] and references therein.

However, SWIPT systems are also vulnerable to potential security issues. This is because RF signals are shared by multiple nodes, which might be potential eavesdroppers. Recent research results show that compared to conventional cryptographic approaches, physical layer security is a better choice in energy and computation constrained systems, such as SWIPT systems [10]. The basic concept behind physical layer security is to exploit the physical layer characteristics of wireless channels to provide perfect secrecy. The work was pioneered by Wyner [11], which confirmed that perfect secrecy can be achieved when the quality of the wiretap channel is a degraded version of the main channel.

Recently, ensuing security in SWIPT systems have gained increasing attentions. In [12], [13], the authors presented the optimal beamforming design and power allocation scheme for multiple-input single-output (MISO) systems in the presence of passive eavesdroppers, later in [14], the issue of uncertain eavesdroppers was tackled, where joint optimization of information and energy beamforming and power allocation were studied. Latest works have considered the security issue in more sophisticated SWIPT systems, such as relay [15], multicast [16], cognitive radio [17] and OFDMA systems [18]. A common of these works is that they consider hybrid network architecture, where the information source also acts as the energy source. However, as analyzed in [19], the

Manuscript received February 24, 2016, revised April 14, 2016, and June 14, 2016, accepted July 11, 2016. This work was supported by the National Key Basic Research Program of China (No. 2012CB316104), the National High-Tech. R&D Program of China under grant 2014AA01A702 and 2014AA01A705, the Zhejiang Provincial Natural Science Foundation of China (LR15F010001), and the Fundamental Research Funds for Central Universities (2016QNA5004). The work of X. Chen was supported by the National Natural Science Foundation of China (No. 61301102). The work of T. Q. Duong was supported by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22. The editor coordinating the review of this paper and approving it for publication was Prof. Z. Ding.

X. Jiang, C. Zhong and Z. Zhang are with the Institute of Information and Communication Engineering, Zhejiang University, China (email: caijunzhong@zju.edu.cn).

X. Chen is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China.(email: chenxiaoming@nuaa.edu.cn).

T. Q. Duong is with ECIT, Queen's University Belfast, Belfast, UK.(email: trung.q.duong@qub.ac.uk).

T. A. Tsiftsis is with the School of Engineering, Nazarbayev University, Astana 01000, Kazakhstan and with TEI of Central Greece, Lamia 35100, Greece (email: Theodoros.tsiftsis@nu.edu.kz).

This paper was presented in part at the European Signal Processing Conference, Budapest, Hungary, August 2016.

harvested energy from hybrid networks is general infeasible to power larger devices such as smartphones, tablets and laptops. Responding to this, a novel network architecture was proposed in [20], where a dedicated station called power beacon (PB) is incorporated into the wireless network to power mobile devices. Very recently, the secrecy performance of device-to-device (D2D) communications in energy harvesting cognitive cellular networks has been investigated in [21], where the D2D transmitter first harvests energy from PBs, then performs secure transmission to the desired D2D receiver.

Thus far, secure communications in SWIPT systems with dedicated PB remain largely an uncharted area. Motivated by this, we consider a point-to-point four-node wirelessly powered wiretap channel consisting of a dedicated PB, an energy constrained information source and a legitimate user in the presence of a passive eavesdropper. It is assumed that the source has no transmit power of its own, hence entirely relies on the external energy charging via wireless power transfer from the PB. For such systems, we present a comprehensive analysis on the achievable secrecy performance. It is worth pointing out that, unlike in the conventional communications systems, where the transmit power is constant, the use of WPT effectively makes the available source transmit power a random variable. In addition, since the transmit power affects both the signals observed at the legitimate user and eavesdropper, the effective signal-to-noise ratios (SNRs) of the main and wiretap channels become correlated, making the secrecy performance analysis much more challenging.

The main contributions of this work can be summarized as follows:

- For enhancing wireless security, we propose simple diversity transmission schemes at the information source, namely, maximum ratio transmission (MRT) and transmit antenna selection (TAS). In particular, for the TAS scheme, depending on the required channel state information (CSI), three different selection criteria are devised.
- For all schemes, closed-form expressions for secrecy outage probability are derived, which enable efficient evaluation of the achievable secrecy performance. Furthermore, simple and informative high SNR approximations are presented. The analytical results suggest that the achievable secrecy performance depends heavily on the available CSI at the source. With the CSI of the main channel, the system attains full secrecy diversity gain, while only unit secrecy diversity order can be achieved with only the CSI of the wiretap channel. In addition, the best performance is achieved when both the CSI of main channel and wiretap channel are available.
- For all schemes, closed-form expressions for average secrecy rate and high SNR approximations are also derived. Our results indicate that, all the schemes attain the same high SNR slope of one and distinct high SNR power offset. Moreover, increasing the number of transmit antennas improves the secrecy rate. However, the gain gradually diminishes when the number of transmit antennas is moderately large.
- Based on the simple high SNR expressions, the optimal time switching ratio θ is studied. It was shown that there exists a unique θ maximizing the secrecy throughput. For the special single-antenna source case, closed-form expression for the optimal θ is obtained.
- We show that, the randomness of source transmit power induced by WPT does not affect the secrecy diversity order and the high SNR slope.

The remainder of the paper is organized as follows. Section II introduces the system model and proposes several transmission schemes. Section III provides an analytical study on the achievable secrecy outage probability of the proposed schemes, while Section IV investigates the average secrecy rate of the system. Numerical results and discussions are presented in Section V. Finally, Section VI concludes the paper and summarizes the key findings.

Notation: We use bold lower case letters to denote vectors and lower case letters to denote scalars; $\|\mathbf{h}\|$ denotes the Frobenius norm; $\mathtt{E}\{x\}$ stands for the expectation of the random variable x and $[x]^+$ denotes $\max(0,x)$; T denotes the transpose operator and $\dagger$ denotes the conjugate operator. $\mathbf{I}_k$ is the identity matrix of size k. $\Gamma(x)$ is the gamma function [22, Eq. (8.31)], $\Gamma(\alpha,x)$ is the upper incomplete gamma function [22, Eq. (8.350.2)] and $\gamma(\alpha,x)$ is the lower incomplete gamma function [22, Eq. (8.350.1)]. $\psi(x)$ denotes the Euler psi function [22, Eq. (8.36)] and $K_v(x)$ is the v-th order modified Bessel function of the second kind [22, Eq. (8.407.1)]. $S_{a,b}(x)$ denotes the Lommel function [22, Eq. (8.570.2)] and $G_{m,n}^{p,q}(x)$ denotes the Meijer G-function [22, Eq. (9.301)].

II. System Model

We consider a four-node wirelessly powered wiretap channel consisting of one PB, one information source Alice and one legitimate user Bob in the presence of one eavesdropper Eve as shown in Fig. 1. We assume that the source is equipped with N antennas, while the other three nodes are equipped with a single antenna.[1] Quasi-static fading is assumed, such that the channel coefficients remain unchanged during each transmission block but vary independently between different blocks.

We adopt the time-sharing protocol proposed in [2]. Hence, a complete transmission slot with time duration of T is divided into two orthogonal sub-slots, i.e., the first one for power transfer with time duration of θT with θ $(0<\theta<1)$ being the time switching ratio, and the second one for information transmission with time duration of $(1-\theta)T$.

During the first phase, the PB sends an energy signal to Alice, and the received energy signal at Alice $\mathbf{y}_s$ can be expressed as

$$\mathbf{y}_s = \sqrt{P_S}\mathbf{h}_P x_s + \mathbf{n}_s, \tag{1}$$

where P_S denotes the transmit power of the PB, x_s is the energy signal with unit power, $\mathbf{n}_s$ is an N-dimensional additive

[1]The considered multi-antenna source model is relevant to the scenarios where an energy constrained multi-antenna sensor node [**?**] transmits confidential information to a single-antenna fusion center or an energy constrained multi-antenna transmitter [24] performs secrecy transmission to a single-antenna receiver.

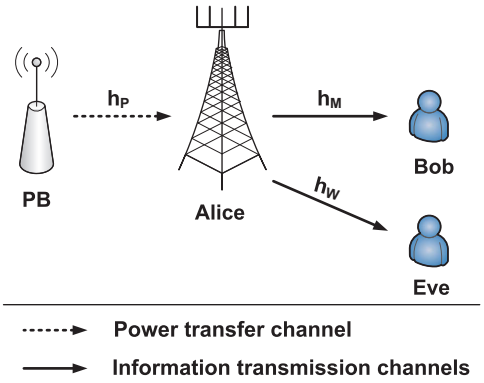


Fig. 1: A schematic diagram of the system model consisting of one PB, one information source Alice, one legitimate user Bob and one eavesdropper Eve.

white Gaussian noise (AWGN) vector with $\mathtt{E}\{\mathbf{n}_s\mathbf{n}_s^\dagger\} = N_0\mathbf{I}$. The $N \times 1$ vector $\mathbf{h}_P$ denotes the power transfer channel from PB to Alice. Due to relatively short distance between the power beacon and the source, it is likely that the line-of-sight propagation exists. Hence, the Nakagami-m distribution is used to model the power transfer channel, i.e., the amplitude of each element of $\mathbf{h}_P$ follows Nakagami-m distribution with shape parameter m and average power λ_P.[2]

Therefore, at the end of the first phase, the total harvested energy within duration θT can be expressed as

$$E = \eta P_S ||\mathbf{h}_P||^2 \theta T, \tag{2}$$

where η $(0 < \eta < 1)$ denotes the energy conversion efficiency.

Since the source communicates with the legitimate user during the second phase with duration $(1-\theta)T$, the transmit power can be computed as

$$P = \frac{E}{(1-\theta)T} = \eta P_S ||\mathbf{h}_P||^2 \frac{\theta}{1-\theta}. \tag{3}$$

To exploit the benefits of multiple antennas at Alice, different transmission schemes can be adopted. In this work, we consider two popular transmission schemes, namely MRT and TAS. The implementation of MRT and TAS requires different types of CSI. For MRT, only the CSI of the main channel is required. While for TAS, partial CSI of the main channel or the wiretap channel is required. In practice, the CSI of the main channel can be estimated at Bob, and then feed back to Alice. On the other hand, the CSI of the wiretap channel can be obtained when the eavesdropper is active in the network, a scenario that is particularly applicable in the networks combining multicast and unicast transmissions where the terminals play dual roles as legitimate receivers for some signals and eavesdroppers for others [25], [26].

A. Maximum Ratio Transmission (MRT)

For the MRT scheme, Alice aims at maximizing the reception quality of the main channel by making use of a channel-match beam, as such, the received signal y_M at Bob can be written as

$$y_M = \sqrt{P}\mathbf{h}_M^T \mathbf{w} x_t + n_M, \tag{4}$$

where x_t denotes the information symbol with unit energy; $N \times 1$ vector $\mathbf{h}_M$ denotes the main channel from Alice to Bob, whose elements are circularly symmetric complex Gaussian random variables (RVs) with zero mean and variance λ_M; n_M denotes the AWGN with zero mean and variance N_0; $\mathbf{w}$ is the MRT vector given by $\mathbf{w} = \frac{\mathbf{h}_M^\dagger}{||\mathbf{h}_M||}$.

Similarly, the signal received at Eve y_W can be expressed as

$$y_W = \sqrt{P}\mathbf{h}_W^T \mathbf{w} x_t + n_W, \tag{5}$$

where the $N \times 1$ vector $\mathbf{h}_W$ denotes the wiretap channel from Alice to Eve, whose elements are circularly symmetric complex Gaussian RVs with zero mean and variance λ_W, and n_W denotes the AWGN with zero mean and variance N_0.

As such, the instantaneous SNR at Bob γ_M and at Eve γ_W are given by

$$\gamma_M^{\mathsf{MRT}} = \frac{\eta P_S ||\mathbf{h}_P||^2 ||\mathbf{h}_M||^2}{N_0} \frac{\theta}{1-\theta}, \tag{6}$$

and

$$\gamma_W^{\mathsf{MRT}} = \frac{\eta P_S ||\mathbf{h}_P||^2 \frac{|\mathbf{h}_W^T \mathbf{h}_M^\dagger|^2}{||\mathbf{h}_M||^2}}{N_0} \frac{\theta}{1-\theta}, \tag{7}$$

respectively.

B. Transmit Antenna Selection (TAS)

TAS is another low-complexity transmission scheme. In this work, we consider three different selection criteria as elaborated below.

1) Criterion 1: In this case, the antenna with the maximum gain of main channel is selected, i.e.,

$$k = \arg \max_{i=1,\cdots,N} |h_{id}|^2, \tag{8}$$

where h_{id} is the i-th element of main channel $\mathbf{h}_M$. It is worth noting that best antenna selection according to the above criterion implies a random antenna selection for the wiretap channel because the main channel is independent of the wiretap channel.

2) Criterion 2: Instead of maximizing the gain of main channel, we now intend to minimize the gain of wiretap channel. As such, the best antenna is selected according to the following criterion:

$$k = \arg \min_{i=1,\cdots,N} |h_{ie}|^2, \tag{9}$$

where h_{ie} is the i-th element of the wiretap channel $\mathbf{h}_W$.

3) Criterion 3: Since the secrecy performance of system depends on the quality of both the main channel and wiretap channel, we now propose the third selection criterion which picks the antenna maximizing the ratio of main channel gain and wiretap channel gain, i.e.,

$$k = \arg \max_{i=1,\cdots,N} \left(\frac{|h_{id}|^2}{|h_{ie}|^2} \right). \tag{10}$$

[2]In the presence of line-of-sight effect, Rician fading is commonly used in literature. However, the analysis with Rician fading is much more involved. As such, for mathematical tractability, we adopt the Nakagami-m fading model, since the Nakagami-m distribution provides very accurate approximation to the Rician distribution.

Hence, the instantaneous SNR at Bob γ_M and at Eve γ_W can be expressed as

$$\gamma_M^{\mathsf{TAS}} = \frac{\eta P_S ||\mathbf{h}_P||^2 |h_{M,k}|^2}{N_0} \frac{\theta}{1-\theta}, \tag{11}$$

and

$$\gamma_W^{\mathsf{TAS}} = \frac{\eta P_S ||\mathbf{h}_P||^2 |h_{W,k}|^2}{N_0} \frac{\theta}{1-\theta}, \tag{12}$$

where $h_{M,k}$ denotes the channel coefficient of the link between the k-th antenna of the source and legitimate user, while $h_{W,k}$ denotes the channel coefficient of the link between the k-th antenna of the source and eavesdropper.

C. Secrecy Performance

For wiretap channels, the secrecy rate C_S is given by the difference of the main channel capacity and the wiretap channel capacity [25]

$$C_S = \begin{cases} \log(1+\gamma_M^\star) - \log(1+\gamma_W^\star) & \gamma_M^\star > \gamma_W^\star, \\ 0 & \gamma_M^\star \leq \gamma_W^\star, \end{cases} \tag{13}$$

where $\star \in \{\mathsf{MRT}, \mathsf{TAS}\}$.

In this work, we consider two different communication scenarios. In the first scenario, Alice uses a constant transmission rate R_S to communicate with Bob. According to [11], perfect secrecy is achievable when $R_S < C_S$, otherwise, secrecy is compromised. In this case, secrecy outage probability becomes an appropriate performance metric. In the second scenario, we assume that Alice adapts its transmission rate according to C_S, as such, ergodic secrecy rate becomes the appropriate performance measure. In the following sections, we present a detailed analysis of the achievable secrecy performance of both MRT and TAS schemes.

III. Secrecy Outage Probability

In this section, we investigate the secrecy outage performance of the considered system. For both transmission schemes, new closed-form expressions for the exact and asymptotic secrecy outage probability are presented. Based on which, the impacts of multiple antennas on the secrecy performance are characterized in terms of the secrecy outage diversity order and the secrecy outage array gain.

According to the definition, the secrecy outage probability can be expressed mathematically as

$$P_{\mathsf{out}}(R_S) = P(C_S < R_S). \tag{14}$$

A. MRT

We start with the MRT scheme, and we have the following key result:

Theorem 1: The exact secrecy outage probability of the MRT scheme can be expressed in closed-form as

$$P_{\mathsf{out}}^{\mathsf{MRT}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \sum_{k=0}^{N-1} \sum_{p=0}^{k} \frac{\lambda_M \left(k_2 \lambda_W\right)^{k-p}}{p! \left(\lambda_M + k_2 \lambda_W\right)^{k-p+1}} \times \left(\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}\right)^{\frac{mN+p}{2}} K_{mN-p}\left(2\sqrt{\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}}\right), \tag{15}$$

where $k_1 = \frac{\eta P_S}{N_0} \frac{\theta}{1-\theta}$ and $k_2 = 2^{R_S}$.

Proof: See Appendix A. ∎

Theorem 1 presents an exact closed-form expression for the secrecy outage probability, which can be efficiently evaluated. However, the expression is too complicated to yield any insights. Motivated by this, we now look into the asymptotic regime, where simple expressions can be obtained. [3]

For the asymptotic high SNR regime, we assume that $\lambda_M \to \infty$ with an arbitrary λ_W. Such a scenario has been widely adopted in the literature, see for instance [27]–[30]. In practice, this occurs when the quality of the main channel is much better than wiretap channel, i.e., Bob is relatively close to Alice while Eve is far away from Alice or the wiretap channel undergoes severe small-scale and large-scale fading effects. In the following, we characterize the two key performance parameters governing the secrecy outage probability in the high SNR regime, i.e., secrecy diversity order G_d and secrecy array gain G_a defined by [31]

$$P_{\mathsf{out}}^{\infty}(R_S) = \left(G_a \lambda_M\right)^{-G_d}. \tag{16}$$

Proposition 1: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of the MRT scheme can be approximated by

$$P_{\mathsf{MRT}}^{\infty}(R_S) = \sum_{k=0}^{N} \frac{1}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1 k_2 \lambda_W \lambda_P}\right)^k \left(\frac{k_2 \lambda_W}{\lambda_M}\right)^N. \tag{17}$$

Proof: See Appendix B. ∎

It is evident from (17) that the system achieves a secrecy diversity order of N. In addition, we observe the intuitive effect of the position of nodes on the secrecy outage probability. For instance, the secrecy outage probability decreases when the PB is close to the source, i.e., large λ_P. It is also easy to see that the high SNR secrecy outage probability $P_{\mathsf{MRT}}^{\infty}(R_S)$ is a decreasing function with respect to $\frac{P_s}{N_0}$, indicating that increasing the transmit power of the PB is always beneficial.

B. TAS Criterion 1

We now move to the TAS Criterion 1 scheme, and we obtain the following key result:

Theorem 2: The exact secrecy outage probability of TAS Criterion 1 scheme can be expressed in closed-form as

$$P_{\mathsf{out}}^{\mathsf{TAS1}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \sum_{k=0}^{N-1} \frac{(-1)^k \binom{N}{k+1} \lambda_M}{\lambda_M + k_2 \lambda_W (k+1)} \times \left(\frac{m(k+1)(k_2-1)}{k_1 \lambda_M \lambda_P}\right)^{\frac{mN}{2}} K_{mN}\left(2\sqrt{\frac{m(k+1)(k_2-1)}{k_1 \lambda_M \lambda_P}}\right). \tag{18}$$

[3] Although the energy transfer efficiency of state of the art technique is low, it is still of both theoretical and practical interests in wirelessly powered communications systems due to the following reasons: First, the energy transfer efficiency can be significantly improved by adopting multiple antenna technology and the PB assisted WPC architecture. Second, the effective SNR could be still reasonably high even if the energy transfer efficiency is low. Third, the key insights obtained from high SNR analysis provide useful guidance for practical system design.

Proof: See Appendix C. ∎

While Theorem 2 presents an exact closed-form expression for the secrecy outage probability, the expression is too complicated to gather more insights. As such, we study the asymptotic behavior for the outage performance.

Proposition 2: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 1 scheme can be approximated as

$$P_{\mathsf{TAS1}}^{\infty}(R_S) = \sum_{k=0}^{N} \frac{N!}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1 k_2 \lambda_W \lambda_P}\right)^k \left(\frac{k_2\lambda_W}{\lambda_M}\right)^N. \quad (19)$$

Proof: When $\lambda_M \to \infty$, we have $\left(1-e^{-\frac{x}{\lambda_M}}\right)^{N-1} = \left(\frac{x}{\lambda_M}\right)^{N-1} + o\left(\left(\frac{x}{\lambda_M}\right)^N\right)$. As such, following the same steps as that of Proposition 1 yields the desired result. ∎

It is evident from (19) that the system also achieves a secrecy diversity order of N. Comparing (17) and (19), we see that $P_{\mathsf{MRC}}^{\infty}(R_S) = \frac{P_{\mathsf{TAS1}}^{\infty}(R_S)}{N!}$, namely, the MRT scheme outperforms the TAS Criterion 1 scheme by a factor of $\frac{1}{N!}$. This is not surprising since the MRT scheme has access to perfect CSI of $\mathbf{h}_M$, while TAS scheme only utilizes partial knowledge of $\mathbf{h}_M$. Recall in the conventional wirelessly powered system without secrecy constraint, the outage probability decays in a much slower speed, i.e., $\rho^{-N}\ln\rho$ instead of ρ^{-N} due to the randomness of the transmit power, where N is the number of antennas, and ρ is the SNR [32], [33]. In the current work, we notice that the randomness of the transmit power does not affect the scaling behavior of the secrecy outage probability. This is because that in wiretap channels, the secrecy performance is determined by the difference between the main and wiretap channel capacities, and the transmit power affects both channels. Hence, the effect of transmit power randomness is canceled.

C. TAS Criterion 2

We now consider the TAS Criterion 2 scheme, and we have the following key result:

Theorem 3: The exact secrecy outage probability of TAS Criterion 2 scheme can be expressed in closed-form as

$$P_{\mathsf{out}}^{\mathsf{TAS2}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \frac{N\lambda_M}{N\lambda_M + k_2\lambda_W} \times \left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN}{2}} K_{mN}\left(2\sqrt{\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}}\right). \quad (20)$$

Proof: See Appendix D. ∎

Having obtained the exact outage probability of TAS Criterion 2 scheme, we now look into the high SNR regime, and derive a simple analytical approximation for the outage probability of the system.

Proposition 3: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 2 scheme can be approximated as

$$P_{\mathsf{TAS2}}^{\infty}(R_S) = \left(\frac{1}{N} + \frac{1}{mN-1}\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)\left(\frac{k_2\lambda_W}{\lambda_M}\right). \quad (21)$$

Proof: See Appendix E. ∎

Different from the previous two cases which achieve a diversity order of N, TAS Criterion 2 scheme only attains unit diversity order. This is also intuitive since TAS Criterion 2 scheme aims to minimize the received SNR of the eavesdropper and the selected antenna serves as a random transmit antenna for the main channel. As such, no secrecy diversity gain can be realized, and increasing the number of antennas N only yields some secrecy array gain.

D. TAS Criterion 3

We now analyze the secrecy outage probability of the system with the TAS Criterion 3 scheme.

Theorem 4: The secrecy outage probability of TAS Criterion 3 scheme can be approximated by

$$P_{\mathsf{out}}^{\mathsf{TAS3}} \approx \left(\frac{k_2}{k_2 + \frac{\lambda_M}{\lambda_W}}\right)^N. \quad (22)$$

Proof: See Appendix F. ∎

Having obtained the outage probability of TAS Criterion 3 scheme, we now look into the asymptotic regime.

Proposition 4: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 3 scheme can be approximated as

$$P_{\mathsf{TAS3}}^{\infty} = \left(\frac{k_2\lambda_W}{\lambda_M}\right)^N. \quad (23)$$

Proof: The proof is straightforward, hence omitted. ∎

As expected, the system achieves a secrecy diversity order of N. Recall the high SNR outage probability of the MRT scheme, and noticing that $\sum_{k=0}^{N}\frac{1}{k!}\frac{\Gamma(mN-k)}{\Gamma(mN)}\left(\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)^k = 1+\sum_{k=1}^{N}\frac{1}{k!}\frac{\Gamma(mN-k)}{\Gamma(mN)}\left(\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)^k > 1$, we observe that the TAS Criterion 3 scheme outperforms the MRT scheme. This is reasonable since the TAS Criterion 3 scheme considers both the CSI of $\mathbf{h}_M$ and $\mathbf{h}_W$, while only the CSI of the $\mathbf{h}_M$ is utilized in the MRT scheme.

E. Optimization of the Time Switching Ratio θ

From the analytical expressions derived in previous subsections, we are ready to study the optimization of time switching ratio θ. Specifically, we adopt the effective secrecy throughput as the performance measure as in [34]. Hence, when the source transmits at a constant rate R_S, the average secrecy throughput can be evaluated by $R = (1-P_{\mathsf{out}})R_S(1-\theta)$. Also, due to space limitation and for illustrative purpose, we only focus on the MRT scheme, while other cases will be numerically illustrated in Section V.

Using the high SNR approximation given in (17), the effective secrecy throughput of the MRT scheme can be expressed

as

$$\tau(\theta) = (1 - P_{\mathsf{MRT}}^{\infty}(\theta))R_S\frac{(1-\theta)T}{T} = (1 - P_{\mathsf{MRT}}^{\infty}(\theta))R_S(1-\theta). \quad (24)$$

Hence, the optimal θ^* is the solution of the following optimization problem:

$$\theta^* = \arg\max_{\theta} \quad \tau(\theta) \quad \text{s.t.} \quad 0 < \theta < 1. \quad (25)$$

To this end, we have the following key result:

Proposition 5: Consider a polynomial

$$\sum_{k=0}^{N} a_k \left(\frac{1-\theta}{\theta}\right)^k (1 + \frac{k}{\theta}) - 1 = 0, \quad (26)$$

where $a_k = \frac{1}{k!}\frac{\Gamma(mN-k)}{\Gamma(mN)}\left(\frac{m(k_2-1)N_0}{\eta P_S k_2 \lambda_P \lambda_W}\right)^k \left(\frac{k_2\lambda_W}{\lambda_M}\right)^N$. Then, the optimal θ^* is the unique root of the polynomial in (0,1).

Proof: Substituting (17) into (24), we obtain

$$\tau(\theta) = \left(1 - \sum_{k=0}^{N} a_k \left(\frac{1-\theta}{\theta}\right)^k\right) b(1-\theta), \quad (27)$$

where $b = R_S$. Thus, the derivative of $\tau(\theta)$ with respect to θ can be expressed as

$$\frac{\mathrm{d}\tau(\theta)}{\mathrm{d}\theta} = \sum_{k=0}^{N} a_k b \left(\frac{1-\theta}{\theta}\right)^k (1 + \frac{k}{\theta}) - b. \quad (28)$$

It is easy to show that $\frac{\mathrm{d}\tau(\theta)}{\mathrm{d}\theta}$ is a monotonically decreasing function with respect to θ. When θ approaches 0, $\frac{\mathrm{d}\tau(\theta)}{\mathrm{d}\theta} \to +\infty$ and when θ approaches 1, $\frac{\mathrm{d}\tau(\theta)}{\mathrm{d}\theta} \to b\left(\frac{2^b\lambda_W}{\lambda_M}\right)^N - b < 0$. Therefore, there exists a unique $\theta^* \in (0,1)$ with $\frac{\mathrm{d}\tau(\theta)}{\mathrm{d}\theta} = 0$, where $\tau(\theta)$ attains its maximum value. ■

In general, due to the complexity of the involved expression, deriving a closed-form solution for θ^* is very challenging. However, for small N, closed-form expressions for θ^* can be obtained.

Remark 1: When $N = 1$, the optimal θ^* is given by

$$\theta^* = \sqrt{\frac{a_1}{1 + a_1 - a_0}}. \quad (29)$$

Remark 2: When $N = 2$, the optimal θ^* is given by

$$\theta^* = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad (30)$$

where $p = \frac{3a_2 - a_1}{1 - a_0 + a_1 - a_2}$ and $q = -\frac{2a_2}{1 - a_0 + a_1 - a_2}$.

F. Comparison of the Proposed Protocols

We now present a more detailed performance comparison for the proposed schemes at the high SNR regime as summarized in Table I on the top of the next page. In general, the secrecy performance depends heavily on the available CSI at the source. The more CSI available, the better the secrecy performance. However, in terms of high SNR protocols investigated shown in Table I. We list the CSI that is required for each protocol and investigate the secrecy diversity order and the outage performance according to the asymptotic secrecy outage probability.

IV. Average Secrecy Rate

In this section, we focus on the average secrecy rate performance of the system. For both transmission schemes, new closed-form expressions for the exact and asymptotic average secrecy rate are presented. Based on which, the impacts of multiple antennas on the secrecy performance are characterized in terms of the high SNR slope and the high SNR power offset.

Starting from the definition, the average secrecy rate can be expressed as

$$\bar{C} = \mathrm{E}\{[\log_2(1+\gamma_M^\star) - \log_2(1+\gamma_W^\star)]^+\}. \quad (31)$$

We now study the achievable secrecy rate of different transmission schemes in the following.

A. MRT

Theorem 5: The exact average secrecy rate of MRT scheme can be expressed in closed-form as (32) on the top of the next page.

Proof: See Appendix G. ■

While (32) provides the exact average secrecy rate, the expression are too complex to yield insightful information. Motivated by this, we now look into the high SNR regime, where the secrecy rate is dictated by two key parameters known as the high SNR slope S_∞ and the high SNR power offset L_∞ [31], i.e.,

$$\bar{C}^\infty = S_\infty(\log_2(\lambda_M) - L_\infty). \quad (33)$$

To this end, we have the following key result:

Proposition 6: For the MRT scheme, the high SNR slope S_∞^{MRT} is given by

$$S_\infty^{\mathsf{MRT}} = 1, \quad (34)$$

and the high SNR power offset L_∞^{MRT} is given by

$$L_\infty^{\mathsf{MRT}} = -\frac{1}{\ln 2}\left(\ln\frac{k_1\lambda_P}{m} + \psi(N) + \psi(mN)\right) + \frac{1}{\Gamma(mN)\ln 2} G_{13}^{31}\left(\frac{m}{k_1\lambda_W\lambda_P}\middle|\begin{matrix}0\\ mN, 0, 0\end{matrix}\right). \quad (35)$$

Proof: See Appendix H. ■

We note that the high SNR slope is also known as the maximum multiplexing gain or the number of degrees of freedom [35]. According to (34), the high SNR slope is one because we assume that the legitimate user only employs a single antenna in this system. In addition, we observe that the wiretap channel only reflects the high SNR power offset. It is also easy to see that the asymptotic average secrecy rate is an increasing function with respect to k_1 and λ_P, indicating that increasing the transmit power of the PB is always beneficial and the secrecy rate increases when PB is close to the source.

TABLE I: Comparison of the proposed schemes

Scheme	CSI requirement	Secrecy diversity order	Outage performance
MRT	$\mathbf{h}_M$	N	Second best
TAS Criterion 1	Index of the entry of $\mathbf{h}_M$	N	Third best
TAS Criterion 2	Index of the entry of $\mathbf{h}_W$	1	Worst
TAS Criterion 3	$\mathbf{h}_M$ and $\mathbf{h}_W$	N	Best

$$\bar{C}^{\mathsf{MRT}} = \frac{1}{\Gamma(mN)\ln 2}\left[\sum_{k=1}^{N-1}\sum_{p=0}^{k-1}(-1)^{k+p+1}\frac{p!}{k!}\left(\frac{m}{k_1\lambda_M\lambda_P}\right)^{k-p-1}\Gamma(mN-k+p+1)\left(1-\frac{1}{\left(1+\frac{\lambda_M}{\lambda_W}\right)^{p+1}}\right)+\right.$$
$$\left.\sum_{k=0}^{N-1}\frac{(-1)^k}{k!}\left(\frac{m}{k_1\lambda_M\lambda_P}\right)^{k}\left(G_{13}^{31}\left(\frac{m\frac{1}{\lambda_M}}{k_1\lambda_P}\middle|\begin{matrix}0\\ mN-k,0,0\end{matrix}\right)-G_{13}^{31}\left(\frac{m(\frac{1}{\lambda_M}+\frac{1}{\lambda_W})}{k_1\lambda_P}\middle|\begin{matrix}0\\ mN-k,0,0\end{matrix}\right)\right)\right]. \quad (32)$$

B. TAS Criterion1

We now consider the TAS Criterion 1 scheme, and we have the following key result:

Theorem 6: The exact average secrecy rate of TAS criterion1 scheme can be expressed in closed-form as (36) on the top of the next page.

Proof: The proof follows similar lines as that of Theorem 5, hence is omitted. ∎

We now look into the high SNR regime, and present the high SNR metrics in the following proposition.

Proposition 7: For the TAS criterion1 scheme, the high SNR slope S_∞^{TAS1} is given by

$$S_\infty^{\mathsf{TAS1}} = 1, \quad (37)$$

and the high SNR power offset L_∞^{TAS1} is given by

$$L_\infty^{\mathsf{TAS1}} = -\frac{1}{\ln 2}\left(\sum_{k=2}^{N}(-1)^k\binom{N}{k}\ln k+\psi(1)+\psi(mN)+\ln\frac{k_1\lambda_P}{m}\right)+\frac{1}{\Gamma(mN)\ln 2}G_{13}^{31}\left(\frac{m}{k_1\lambda_W\lambda_P}\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right). \quad (38)$$

Proof: The proof follows similar lines as that of Proposition 6, hence is omitted. ∎

C. TAS Criterion2

We now analyze the average secrecy rate of the system with the TAS Criterion 2 scheme, and we have the following key result:

Theorem 7: The exact average secrecy rate of TAS criterion2 scheme can be expressed in closed-form as

$$\bar{C}^{\mathsf{TAS2}} = \frac{1}{\Gamma(mN)\ln 2}\left[G_{13}^{31}\left(\frac{m}{k_1\lambda_P}\frac{1}{\lambda_M}\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right)-G_{13}^{31}\left(\frac{m}{k_1\lambda_P}(\frac{1}{\lambda_M}+\frac{N}{\lambda_W})\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right)\right]. \quad (39)$$

Proof: The proof follows similar lines as that of Theorem 5, hence is omitted. ∎

Having obtained the exact average secrecy rate of TAS Criterion 2 scheme, we now look into the asymptotic regime.

Proposition 8: For the TAS criterion2 scheme, the high SNR slope S_∞^{TAS2} is given by

$$S_\infty^{\mathsf{TAS2}} = 1, \quad (40)$$

and the high SNR power offset L_∞^{TAS2} is given by

$$L_\infty^{\mathsf{TAS2}} = -\frac{1}{\ln 2}\left(\ln\frac{k_1\lambda_P}{m}+\psi(1)+\psi(mN)\right)+\frac{1}{\Gamma(mN)\ln 2}G_{13}^{31}\left(\frac{mN}{k_1\lambda_W\lambda_P}\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right). \quad (41)$$

Proof: The proof follows similar lines as that of Proposition 6, hence is omitted. ∎

D. TAS Criterion3

We now move to the TAS Criterion 3 scheme, and we obtain the following key result:

Theorem 8: The average secrecy rate of TAS criterion3 scheme can be approximated by

$$\bar{C}^{\mathsf{TAS3}} \approx \frac{1}{\ln 2}\frac{\lambda_M}{\lambda_W}\sum_{k=0}^{N-1}\frac{1}{\Gamma(k+1)\Gamma(N-k)}\times G_{33}^{23}\left(1+\frac{\lambda_M}{\lambda_W}\middle|\begin{matrix}-N,1+k-N,1+k-N\\ 0,1+k-N,k-N\end{matrix}\right). \quad (42)$$

Proof: See Appendix I. ∎

We now look into the high SNR regime, and present the high SNR metrics in the following proposition.

Proposition 9: For the TAS criterion3 scheme, the high SNR slope S_∞^{TAS3} is given by

$$S_\infty^{\mathsf{TAS3}} = 1, \quad (43)$$

and the high SNR power offset L_∞^{TAS3} is given by

$$L_\infty^{\mathsf{TAS3}} = \frac{1}{\ln 2}\left(\ln\lambda_W+\frac{1}{N}-N+\sum_{k=2}^{N}(-1)^k\binom{N}{k}\frac{1}{k}\right). \quad (44)$$

Proof: See Appendix J. ∎

$$\bar{C}^{\mathsf{TAS1}} = \frac{1}{\Gamma(mN)\ln 2}\sum_{k=1}^{N}(-1)^{k+1}\binom{N}{k}\left[G_{13}^{31}\left(\frac{m}{k_1\lambda_P}\frac{k}{\lambda_M}\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right) - G_{13}^{31}\left(\frac{m}{k_1\lambda_P}(\frac{k}{\lambda_M}+\frac{1}{\lambda_W})\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right)\right]. \quad (36)$$

V. Numerical Results

In this section, we present numerical results to verify the theoretical expressions. Unless otherwise stated, we set the source transmission rate as $R_S = 1$ bit/s/Hz, the energy conversion efficiency as $\eta = 0.8$ and the time switching ratio as $\theta = 0.5$. The Nakagami-m parameter is set to be $m = 4$, which corresponds to a Rician factor of $K = 3 + \sqrt{12}$. The transmit power of the PB to the noise ratio as $\frac{P_S}{N_0} = 10$ dB, the channel variance as $\lambda_P = 1$ and $\lambda_W = 10$. Also, we set $\rho = \frac{P_S}{N_0}\lambda_M$ and $\rho_1 = \frac{P_S}{N_0}\lambda_W$ to denote the average SNR of the main channel and the wiretap channel, respectively.

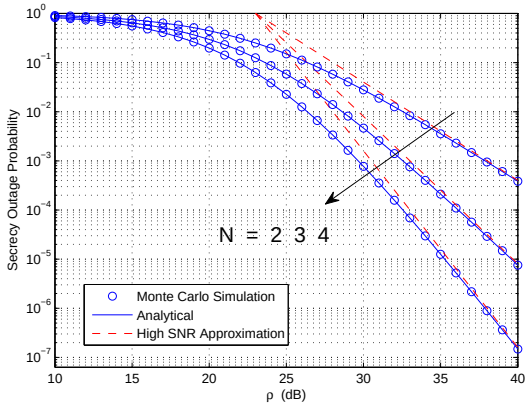


Fig. 2: Secrecy outage probability versus ρ with different N for the MRT scheme.

Fig. 2 plots the secrecy outage probability versus ρ with different N for the MRT scheme. As illustrated, the analytical results are in exact agreement with the Monte Carlo simulations, which demonstrates the correctness of the analytical expression. In addition, the high SNR results accurately predict the secrecy diversity order and the secrecy array gain, and increasing N substantially enhances the secrecy outage performance by achieving a higher secrecy diversity gain.

Fig. 3 illustrates the secrecy outage probability of three different TAS schemes. Once again, we observe that the analytical curves are in perfect agreement with the Monte Carlo simulation results and the high SNR approximation are sufficiently tight for all curves. As expected, the TAS Criterion 2 scheme only attains unit diversity order, while the other two TAS schemes achieves a full diversity order of N. In addition, it is observed that the TAS Criterion 3 scheme yields the best secrecy outage performance. However, the TAS Criterion 2 scheme tends to outperform the TAS Criterion 1 scheme in the low SNR regime, and then becomes inferior as the operating SNR becomes sufficiently high.

Fig. 4 examines the average secrecy rate of the MRT scheme. We observe that the high SNR slope of all the curves is one, which corroborates the theoretical analysis presented

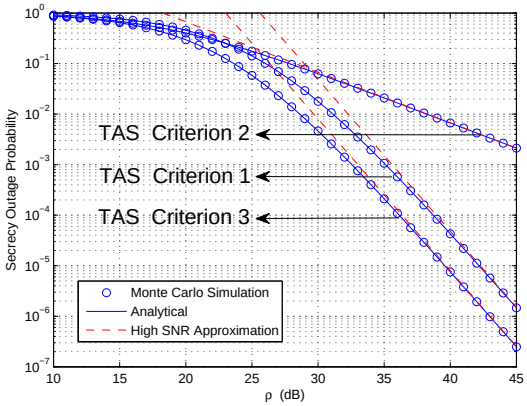


Fig. 3: Secrecy outage probability versus ρ for different TAS schemes with $N = 3$.

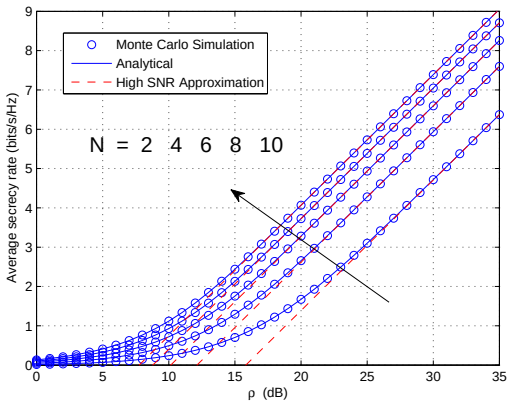


Fig. 4: Average secrecy rate versus ρ with different N for the MRT scheme.

in previous section. Nevertheless, increasing N improves the average secrecy rate by decreasing the high SNR power offset. However, the benefit of increasing the number of antennas N gradually diminishes when N is sufficiently large.

Fig. 5 investigates the impact of distance between Alice and Eve on the average secrecy rate for different TAS schemes. As expected, the TAS Criterion 3 scheme always attains the best performance. At the low ρ_1 regime, namely, relatively large distance between Alice and Eve (or small λ_W), the TAS Criterion 1 scheme outperforms the TAS Criterion 2 scheme. However, the opposite holds when the distance decreases, i.e., λ_W becomes large. This phenomenon is quite intuitive, since when the average channel gain of the wiretap channel is better than that of the main channel, selecting the worst antenna as per the TAS Criterion 2 scheme substantially degrades the capacity of the wiretap channel, thereby resulting in a larger secrecy performance gain than the TAS Criterion 1 scheme.

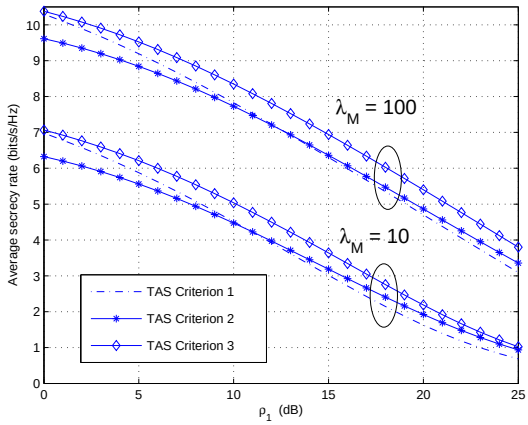


Fig. 5: Average secrecy rate versus ρ_1 for different TAS schemes with $N = 3$.

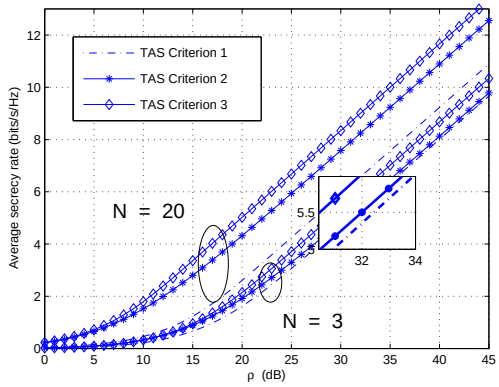
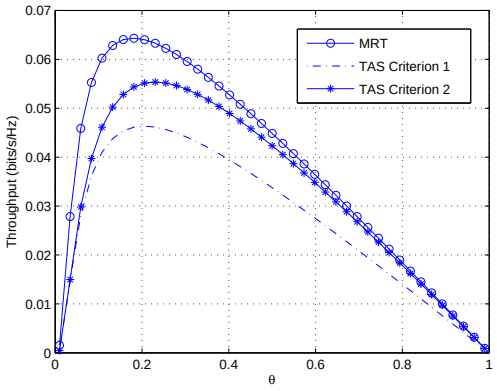
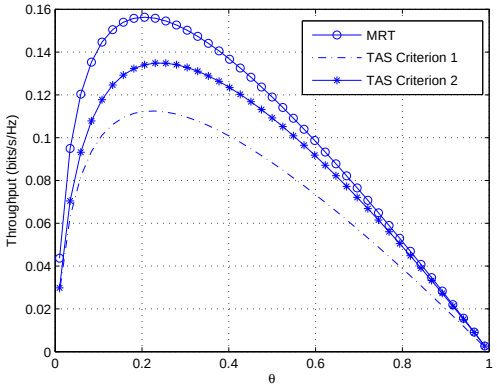


Fig. 6: Average secrecy rate versus ρ for different TAS schemes.



(a) $R(\theta) = (1 - P_{\text{out}})R_S(1 - \theta)$



(b) $R(\theta) = (1 - \theta)\bar{C}$

Fig. 7: Effective throughput versus θ for different schemes with $N = 2$ and $\lambda_M = 1$.

Fig. 6 compares the average secrecy rate for different TAS schemes. Once again, we observe that the high SNR slopes are one. The TAS Criterion 2 scheme outperforms the TAS Criterion 1 scheme with a large λ_W. In addition, the number of antennas N has a significant impact on the performance of TAS schemes. For small N, i.e., $N = 3$, all the three TAS schemes attain similar secrecy rate. While for large N, i.e., $N = 20$, the secrecy rate difference becomes much more pronounced.

Fig. 7 depicts the impact of time split parameter θ on the secrecy performance of different schemes. Specifically, we adopt the effective throughput as the performance measure as in [34]. Hence, when the source transmits at a constant rate R_S, the average throughput can be evaluated by $R = (1 - P_{\text{out}})R_S(1 - \theta)$, while when the source transmits at a varying rate adapting to the secrecy rate, the throughput is given by $R = (1 - \theta)\bar{C}$. It is observed that, in all cases, the effective throughput first increases along with θ, and then start to decrease after reaching the maximum point, indicating that there exists a unique optimal time split parameter θ. In addition, we see that, with optimized time split parameter θ, the MRT scheme achieves the highest throughput as expected. Also, it is observed that the TAS Criterion 2 scheme outperforms the TAS Criterion 1. The reason is that we have set $\lambda_M = 1$ and $\lambda_W = 10$ in the simulations, a scenario where the average gain of the main channel is worse than the wiretap channel. Hence, the main channel capacity enhancement due to selection of the strongest channel in TAS Criterion 1 scheme is rather insignificant compared to the wiretap channel capacity degradation due to the selection of the weakest channel in TAS Criterion 2 scheme.

VI. Conclusion

In this paper, we have investigated the secrecy performance of the wirelessly powered wiretap channels. For both MRT and TAS schemes, exact analytical expressions and asymptotic approximations are presented, which facilitate the extraction of key insights of the achievable secrecy outage probability and average secrecy rate performance. The findings of the paper suggest that, with CSI of the main channel (e.g., MRT and TAS Criteria 1 and 3), the system can achieve substantial secrecy diversity gain. On the other hand, without the CSI of the main channel (e.g., TAS Criterion 2), no diversity gain can be attained, which indicates the critical importance of CSI in the design of practical systems.

APPENDIX A
PROOF OF THEOREM 1

We start by expressing the SNR given in (6) and (7) as

$$\gamma_M^{\mathsf{MRT}} = k_1 y_{h_P} y_{h_M}, \quad \text{and} \quad \gamma_W^{\mathsf{MRT}} = k_1 y_{h_P} y_{h_W}, \tag{45}$$

where $k_1 = \frac{\eta P_S}{N_0}\frac{\theta}{1-\theta}$, $y_{h_P} = ||\mathbf{h}_P||^2$, $y_{h_M} = ||\mathbf{h}_M||^2$ and $y_{h_W} = \frac{|\mathbf{h}_W^T \mathbf{h}_M|^2}{||\mathbf{h}_M||^2}$. It is straightforward to show that the probability density function (pdf) of y_{h_P} follows a gamma distribution with shape parameter mN and scale parameter λ_P/m given by [36]

$$f_{y_{h_P}}(x) = \frac{1}{\Gamma(mN)}\left(\frac{m}{\lambda_P}\right)^{mN} x^{mN-1} e^{-\frac{m}{\lambda_P}x}, \tag{46}$$

and the pdf of y_{h_M} follows a chi-square distribution with $2N$ degrees of freedom given by [37]

$$f_{y_{h_M}}(x) = \frac{x^{N-1}}{\lambda_M^N \Gamma(N)} e^{-\frac{x}{\lambda_M}}. \tag{47}$$

In addition, according to [38], y_{h_W} follows an exponential distribution with pdf

$$f_{y_{h_W}}(x) = \frac{1}{\lambda_W} e^{-\frac{x}{\lambda_W}}, \tag{48}$$

and is independent of y_{h_M}. As such, the secrecy outage probability can be written as

$$P_{\mathsf{out}}^{\mathsf{MRT}}(R_S) = 1 - P\left(\frac{1 + k_1 y_{h_P} y_{h_M}}{1 + k_1 y_{h_P} y_{h_W}} \geq k_2\right), \tag{49}$$

where $k_2 = 2^{R_S}$. Conditioned on y_{h_P} and y_{h_W}, with the help of [22, Eq. (3.351.2)], we obtain

$$\begin{aligned} P_{\mathsf{out}}^{\mathsf{MRT}}(R_S|y_{h_P}, y_{h_W}) &= 1 - \int_{\frac{k_2-1}{k_1 y_{h_P}} + k_2 y_{h_W}}^{\infty} \frac{x^{N-1}}{\lambda_M^N \Gamma(N)} e^{-\frac{x}{\lambda_M}} \mathrm{dx} \\ &= 1 - e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}} - \frac{k_2 y_{h_W}}{\lambda_M}} \sum_{k=0}^{N-1} \frac{1}{k!}\left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}} + \frac{k_2 y_{h_W}}{\lambda_M}\right)^k. \end{aligned} \tag{50}$$

By applying the binomial expansion $(x_1 + x_2)^n = \sum_{k=0}^{n} \binom{n}{k} {x_1}^k {x_2}^{n-k}$, (50) can be further expressed as

$$\begin{aligned} P_{\mathsf{out}}^{\mathsf{MRT}}(R_S|y_{h_P}, y_{h_W}) &= 1 - \sum_{k=0}^{N-1} \sum_{p=0}^{k} \frac{1}{p!(k-p)!} \times \\ & e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}}} \left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}}\right)^p e^{-\frac{k_2 y_{h_W}}{\lambda_M}} \left(\frac{k_2 y_{h_W}}{\lambda_M}\right)^{k-p}. \end{aligned} \tag{51}$$

Noticing that the RV y_{h_P} is decoupled with y_{h_W}, the expectation can be taken separately. Hence, with the help of [22, Eq. (3.471.9)], we obtain

$$\begin{aligned} &\int_0^{\infty} e^{-\frac{k_2-1}{k_1 \lambda_M x}} \left(\frac{k_2-1}{k_1 \lambda_M x}\right)^p \frac{x^{mN-1}}{\Gamma(mN)} \left(\frac{m}{\lambda_P}\right)^{mN} e^{-\frac{m}{\lambda_P}x} \mathrm{dx} = \\ &\frac{2}{\Gamma(mN)} \left(\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}\right)^{\frac{mN+p}{2}} K_{mN-p}\left(2\sqrt{\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}}\right). \end{aligned} \tag{52}$$

Similarly, invoking [22, Eq. (3.326.2)], we have

$$\int_0^{\infty} e^{-\frac{k_2 x}{\lambda_M}} \left(\frac{k_2 x}{\lambda_M}\right)^{k-p} \frac{e^{-\frac{x}{\lambda_W}}}{\lambda_W} \mathrm{dx} = \frac{(k-p)! \lambda_M \left(k_2 \lambda_W\right)^{k-p}}{\left(\lambda_M + k_2 \lambda_W\right)^{k-p+1}}. \tag{53}$$

To this end, pulling everything together yields the desired result.

APPENDIX B
PROOF OF PROPOSITION 1

Starting from (49), conditioned on y_{h_P} and y_{h_M}, we have

$$\begin{aligned} &P_{\mathsf{out}}^{\mathsf{MRT}}(R_S|y_{h_P}, y_{h_M}) = 1 - \\ &\mathrm{Prob}\left(y_{h_M} > \frac{k_2-1}{k_1 y_{h_P}}\right) \times \int_0^{\frac{y_{h_M}}{k_2} - \frac{k_2-1}{k_1 k_2 y_{h_P}}} \frac{1}{\lambda_W} e^{-\frac{x}{\lambda_W}} \mathrm{dx} \\ &= 1 - \mathrm{Prob}\left(y_{h_M} > \frac{k_2-1}{k_1 y_{h_P}}\right) \times \left(1 - e^{-\frac{y_{h_M}}{k_2 \lambda_W} + \frac{k_2-1}{k_1 k_2 \lambda_W y_{h_P}}}\right). \end{aligned} \tag{54}$$

With the help of [22, Eq. (3.351.2)] and $e^{\frac{k_2-1}{k_1 \lambda_M y_{h_P}}} = \sum_{k=0}^{\infty} \frac{1}{k!}\left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}}\right)^k$, conditioned on y_{h_P}, the outage probability can be expressed as

$$\begin{aligned} P_{\mathsf{out}}^{\mathsf{MRT}}(R_S|y_{h_P}) = e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}}} \sum_{k=N}^{\infty} \frac{1}{k!}\left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}}\right)^k + \\ e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}}} \sum_{k=0}^{N-1} \frac{1}{k!} \frac{\left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}}\right)^k}{\left(1 + \frac{\lambda_M}{k_2 \lambda_W}\right)^{N-k}}. \end{aligned} \tag{55}$$

Then, averaging over y_{h_P}, with the help of [22, Eq. (3.471.9)], the secrecy outage probability can be computed as (56) on the top of next page.

Expanding the Bessel function by [22, Eq. (8.446)] and omitting the high order items yield

$$\begin{aligned} P_{\mathsf{MRT}}^{\infty}(R_S) = \sum_{k=N}^{\infty} \frac{1}{k!}\left(\frac{m(k_2-1)}{k_1 \lambda_M \lambda_P}\right)^k \frac{\Gamma(mN-k)}{\Gamma(mN)} + \\ \sum_{k=0}^{N-1} \frac{1}{k!} \frac{\left(\frac{m(k_2-1)}{k_1 \lambda_M \lambda_P}\right)^k}{\left(1 + \frac{\lambda_M}{k_2 \lambda_W}\right)^{N-k}} \frac{\Gamma(mN-k)}{\Gamma(mN)}. \end{aligned} \tag{57}$$

By omitting the high order items, the desired result can be obtained.

APPENDIX C
PROOF OF THEOREM 2

Based on (11) and (12), we set $y_{h_M} = |h_{M,k}|^2$ and $y_{h_W} = |h_{W,k}|^2$. In this case, since the selected antenna corresponds to a random transmit antenna for the eavesdropper, the pdf of y_{h_W} can be expressed as $f_{y_{h_W}}(x) = \frac{1}{\lambda_W} e^{-\frac{x}{\lambda_W}}$. Now, with some simple algebraic manipulations, the cumulative distribution function (cdf) of y_{h_M} can be shown as

$$F_{y_{h_M}}(x) = \left(\int_0^x \frac{1}{\lambda_M} e^{-\frac{t}{\lambda_M}} \mathrm{dt}\right)^N = \left(1 - e^{-\frac{x}{\lambda_M}}\right)^N. \tag{58}$$

$$P_{\text{out}}^{\text{MRT}}(R_S)=\sum_{k=N}^{\infty}\frac{1}{k!}\left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^k\frac{2}{\Gamma(mN)}\left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN-k}{2}}K_{mN-k}\left(2\sqrt{\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}}\right)+$$
$$\sum_{k=0}^{N-1}\frac{1}{k!}\frac{\left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^k}{\left(1+\frac{\lambda_M}{k_2\lambda_W}\right)^{N-k}}\frac{2}{\Gamma(mN)}\left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN-k}{2}}K_{mN-k}\left(2\sqrt{\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}}\right). \quad (56)$$

Hence the pdf of y_{h_M} can be obtained with a simple derivative as follows:

$$f_{y_{h_M}}(x)=\frac{N}{\lambda_M}\left(1-e^{-\frac{x}{\lambda_M}}\right)^{N-1}e^{-\frac{x}{\lambda_M}}. \quad (59)$$

Then, the desired result can be obtained by following similar lines as in the proof of Theorem 1.

Appendix D
Proof of Theorem 3

In this case, the strongest antenna corresponds to a random transmit antenna for the legitimate user, as such, the pdf of y_{h_M} can be expressed as $f_{y_{h_M}}(x)=\frac{1}{\lambda_M}e^{-\frac{x}{\lambda_M}}$. Then, with some simple algebraic manipulations, the cdf of y_{h_W} can be shown as

$$F_{y_{h_W}}(x)=1-\left(\int_x^{\infty}\frac{1}{\lambda_W}e^{-\frac{t}{\lambda_W}}\,\mathrm{dt}\right)^N=1-e^{-\frac{N}{\lambda_W}x}. \quad (60)$$

Taking derivation of (60), the pdf of y_{h_W} can be expressed as

$$f_{y_{h_W}}(x)=\frac{N}{\lambda_W}e^{-\frac{N}{\lambda_W}x}. \quad (61)$$

Then, the desired result can be obtained by following similar lines as in the proof of Theorem 1.

Appendix E
Proof of Proposition 3

By following the same steps as in the proof of Proposition 1, we obtain

$$P_{\text{out}}^{\text{TAS2}}(R_S)=1-\frac{N\lambda_M}{N\lambda_M+k_2\lambda_W}\frac{2}{\Gamma(mN)}\times$$
$$\left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN}{2}}K_{mN}\left(2\sqrt{\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}}\right). \quad (62)$$

Expanding the Bessel function and omitting the high order items yield

$$P_{\text{out}}^{\text{TAS2}}(R_S)=1-\frac{N\lambda_M}{N\lambda_M+k_2\lambda_W}\times$$
$$\left(1-\frac{m(k_2-1)}{(mN-1)k_1\lambda_P}\frac{1}{\lambda_M}+o\left(\frac{1}{\lambda_M^2}\right)\right). \quad (63)$$

Then, the desired result can be obtained along with some simple algebraic manipulations.

Appendix F
Proof of Theorem 4

The exact secrecy outage probability is difficult to characterize, instead, we apply the following approximation as in [39]

$$C_S=\left[\log\left(\frac{1+\gamma_M}{1+\gamma_W}\right)\right]^+$$
$$\approx\left[\log\left(\frac{\gamma_M}{\gamma_W}\right)\right]^+=\left[\log\left(\frac{|h_{M,k}|^2}{|h_{W,k}|^2}\right)\right]^+. \quad (64)$$

It is worth pointing out that, such approximation is reasonably tight and becomes asymptotically exact in the high SNR regime.

Then, we can define a new variable as follows

$$X=\max_{i=1,\cdots,N}\left(\frac{|h_{id}|^2}{|h_{ie}|^2}\right). \quad (65)$$

Along with some simple algebraic manipulations, the cdf of X can be computed as

$$F_X(x)=\left(\int_0^{\infty}\int_{\frac{y}{x}}^{\infty}\frac{1}{\lambda_W}e^{-\frac{t}{\lambda_W}}\frac{1}{\lambda_M}e^{-\frac{y}{\lambda_M}}\,\mathrm{dtdy}\right)^N$$
$$=\left(\frac{x}{x+\frac{\lambda_M}{\lambda_W}}\right)^N. \quad (66)$$

Taking derivation of (66), the pdf of X can be expressed as

$$f_X(x)=N\frac{\lambda_M}{\lambda_W}\frac{x^{N-1}}{\left(x+\frac{\lambda_M}{\lambda_W}\right)^{N+1}}. \quad (67)$$

To this end, the desired result can be expressed as $F_X(k_2)$.

Appendix G
Proof of Theorem 5

Starting from (31), conditioned on y_{h_P}, by following the same steps as in [31], we formulate the average secrecy rate as

$$\bar{C}^{\text{MRT}}=\frac{1}{\ln 2}\int_0^{\infty}\frac{k_1y_{h_P}}{1+k_1y_{h_P}x}F_{y_{h_W}}(x)\left(1-F_{y_{h_M}}(x)\right)\mathrm{dx}$$
$$=\frac{1}{\ln 2}\int_0^{\infty}\frac{k_1y_{h_P}}{1+k_1y_{h_P}x}\left(1-e^{-\frac{x}{\lambda_W}}\right)\frac{\Gamma\left(N,\frac{x}{\lambda_M}\right)}{\Gamma(N)}\mathrm{dx}. \quad (68)$$

Invoking [22, Eq. (3.383.10)] and expanding the incomplete Gamma function, the average secrecy rate can be computed

$$\bar{C}^{\mathsf{MRT}} = \frac{1}{\ln 2}\sum_{k=0}^{N-1}\left(\frac{1}{k_1\lambda_M y_{h_P}}\right)^k \frac{(-1)^k}{k!}\left(e^{\frac{\frac{1}{\lambda_M}}{k_1 y_{h_P}}}\Gamma\left(0,\frac{\frac{1}{\lambda_M}}{k_1 y_{h_P}}\right) - e^{\frac{\frac{1}{\lambda_M}+\frac{1}{\lambda_W}}{k_1 y_{h_P}}}\Gamma\left(0,\frac{\frac{1}{\lambda_M}+\frac{1}{\lambda_W}}{k_1 y_{h_P}}\right)\right) - \frac{1}{\ln 2}\sum_{k=1}^{N-1}\sum_{p=0}^{k-1}(-1)^{k+p}\left(\frac{1}{k_1\lambda_M y_{h_P}}\right)^k \frac{p!}{k!}\left(\left(\frac{k_1 y_{h_P}}{\frac{1}{\lambda_M}}\right)^{p+1} - \left(\frac{k_1 y_{h_P}}{\frac{1}{\lambda_M}+\frac{1}{\lambda_W}}\right)^{p+1}\right). \quad (69)$$

as (69) on the top of the page.

The next step is to average over y_{h_P}. Here, we set

$$A = \frac{1}{\ln 2}\sum_{k=0}^{N-1}\left(\frac{1}{k_1\lambda_M}\right)^k \frac{(-1)^k}{k!}\frac{1}{\Gamma(mN)}\left(\frac{m}{\lambda_P}\right)^{mN} \times \int_0^\infty x^{mN-k-1} e^{-\frac{m}{\lambda_P}x+\frac{1}{k_1\lambda_M x}}\Gamma\left(0,\frac{1}{k_1\lambda_M x}\right)\mathrm{dx}. \quad (70)$$

With the help of [22, Eq. (8.353.3)] and [22, Eq. (3.471.9)], (70) can be further expressed as

$$A = \frac{1}{\ln 2}\sum_{k=0}^{N-1}\left(\frac{1}{k_1\lambda_M}\right)^k \frac{(-1)^k}{k!}\frac{1}{\Gamma(mN)}\left(\frac{m}{\lambda_P}\right)^{\frac{mN+k}{2}} \times \int_0^\infty \frac{4x^{mN-k+1}}{x^2+\frac{1}{k_1\lambda_M}} K_{mN-k}\left(2x\sqrt{\frac{m}{\lambda_P}}\right)\mathrm{dx}. \quad (71)$$

Invoking [22, Eq. (6.565.7)], we have

$$A = \sum_{k=0}^{N-1}\frac{(-1)^k}{\ln 2}\frac{\Gamma(mN-k+1)}{\Gamma(mN)k!}\left(\frac{m}{k_1\lambda_M\lambda_P}\right)^k 2^{mN-k+2} \times \left(\frac{m}{k_1\lambda_M\lambda_P}\right)^{\frac{mN-k}{2}} S_{-1-mN+k,mN-k}\left(2\sqrt{\frac{m}{k_1\lambda_M\lambda_P}}\right). \quad (72)$$

With the help of [22, Eq. (9.34.6)] and [22, Eq. (9.31.5)], we obtain

$$A = \frac{1}{\ln 2}\sum_{k=0}^{N-1}\frac{(-1)^k}{k!}\frac{1}{\Gamma(mN)}\left(\frac{m}{k_1\lambda_M\lambda_P}\right)^k \times G_{13}^{31}\left(\frac{m}{k_1\lambda_M\lambda_P}\middle|\begin{matrix}0\\ mN-k,0,0\end{matrix}\right). \quad (73)$$

To this end, by following the same steps and utilizing [22, Eq. (3.326.2)], the desired result can be obtained.

Appendix H
Proof of Proposition 6

Capitalizing on the general framework proposed in [31] for the evaluation of asymptotic average secrecy rate, conditioned on y_{h_P}, we have

$$\bar{C}^{\infty} = A - B = \frac{1}{\ln 2}\int_0^\infty \ln(k_1 y_{h_P} x) f_{y_{h_M}}(x)\mathrm{dx} - \frac{1}{\ln 2}\int_0^\infty \frac{k_1 y_{h_P}}{1+k_1 y_{h_P} x}\left(1-F_{y_{h_W}}(x)\right)\mathrm{dx}. \quad (74)$$

With the help of [22, Eq. (4.352.1)], A can be computed as

$$A = \log_2(\lambda_M) + \frac{1}{\ln 2}\left(\ln\frac{k_1\lambda_P}{m} + \psi(N) + \psi(mN)\right). \quad (75)$$

The calculation of B is exactly the same as $\bar{C}$ above. Then we have

$$B = \frac{1}{\Gamma(mN)\ln 2}G_{13}^{31}\left(\frac{m}{k_1\lambda_W\lambda_P}\middle|\begin{matrix}0\\ mN,0,0\end{matrix}\right). \quad (76)$$

The desired result then follows immediately.

Appendix I
Proof of Theorem 8

Starting from the definition, we have

$$\bar{C}^{\mathsf{TAS3}} = \int_1^\infty \log(x) f_X(x)\mathrm{dx}. \quad (77)$$

Substituting (67) into (77) yields

$$\bar{C}^{\mathsf{TAS3}} = \frac{N}{\ln 2}\frac{\lambda_M}{\lambda_W}\int_1^\infty \ln x \frac{x^{N-1}}{\left(x+\frac{\lambda_M}{\lambda_W}\right)^{N+1}}\mathrm{dx}. \quad (78)$$

Making a change of variable $t = x-1$ and utilizing [40, Eq. (8.4.6.5)], (78) can be alternatively written as

$$\bar{C}^{\mathsf{TAS3}} = \frac{N}{\ln 2}\frac{\lambda_M}{\lambda_W}\int_0^\infty \ln(t+1)\frac{(t+1)^{N-1}}{\left(t+1+\frac{\lambda_M}{\lambda_W}\right)^{N+1}}\mathrm{dt} = \frac{N}{\ln 2}\frac{\lambda_M}{\lambda_W}\int_0^\infty G_{22}^{12}\left(t\middle|\begin{matrix}1,1\\ 1,0\end{matrix}\right)\frac{(t+1)^{N-1}}{\left(t+1+\frac{\lambda_M}{\lambda_W}\right)^{N+1}}\mathrm{dt}. \quad (79)$$

Applying the binomial expansion and utilizing [22, Eq. (7.811.5)] yield the desired result.

Appendix J
Proof of Proposition 9

By taking the general form, we obtain

$$\bar{C}^{\infty} = A - B = \frac{1}{\ln 2}\int_0^\infty \ln(x) f_{y_{h_M}}(x)\mathrm{dx} - \frac{1}{\ln 2}\int_0^\infty \ln(y) f_{y_{h_W}}(y)\mathrm{dy}, \quad (80)$$

where the two pdfs $f_{y_{h_M}}(x)$ and $f_{y_{h_W}}(x)$ have been derived in [41] as

$$f_{y_{h_M}}(x) = \frac{Nx^{N-1}}{\lambda_M^N}\Gamma(2-N,\frac{x}{\lambda_M}), \quad (81)$$

and

$$f_{y_{h_W}}(x) = N(N-1)\times \sum_{k=0}^{N-2}(-1)^k\binom{N-2}{k}\frac{x^{k+1}}{\lambda_W^{k+2}}\Gamma\left(-1-k,\frac{x}{\lambda_W}\right). \quad (82)$$

For A, by utilizing [22, Eq. (8.350.2)] and [22, Eq. (4.352.1)], we obtain

$$A = \frac{1}{\ln 2}\left(\ln\lambda_M + \psi(2) - \frac{1}{N}\right). \quad (83)$$

Following the similar lines, B can be computed as

$$B = \frac{1}{\ln 2}\left(\ln\lambda_W + \psi(1) + 1 - N + \sum_{k=2}^{N}(-1)^k\binom{N}{k}\frac{1}{k}\right). \quad (84)$$

The desired result then follows immediately.

REFERENCES

[1] R. Zhang and C. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[2] A. A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.

[3] L. Liu, R. Zhang, and K. Chua, "Wireless infomation and power transfer: A dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, Sep. 2013.

[4] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, Oct. 2014.

[5] Z. Ding, S. M. Perlaza, I. Esnaola, and H. V. Poor, "Power allocation strategies in energy harvesting wireless cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 846–860, Feb. 2014.

[6] Z. Ding, C. Zhong, D. Ng, M. Peng, H. A. Suraweera, R. Schober, and H. V. Poor, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, Apr. 2015.

[7] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchoa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.

[8] C. Zhong, G. Zheng, Z. Zhang, and G. Karagiannids, "Optimum wirelessly powered relaying," *IEEE Signal Processing Lett.*, vol. 22, no. 10, pp. 1728–1732, Oct. 2015.

[9] K. Huang, C. Zhong, and G. Zhu, "Some new research trends in wirelessly powered communications," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 19–27, 2016.

[10] S. Bi, C. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 117–125, Apr. 2015.

[11] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[12] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[13] H. Zhang, C. Li, Y. Huang, and L. Yang, "Secure beamforming for SWIPT in multiuser MISO broadcast channel with confidential messages," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1347–1350, Aug. 2015.

[14] D. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[15] Q. Li, Q. Zhang, and J. Qin, "Secure relay breamforming for simulatneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, June 2014.

[16] B. Zhu, J. Ge, Y. Huang, Y. Yang, and M. Lin, "Rank-two beamformed secure multicasting for wireless information and power transfer," *IEEE Signal Process. Lett.*, vol. 21, no. 2, pp. 199–203, Feb. 2014.

[17] D. Ng, E. S. Lo, and R. Schober, "Multiobjective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3166–3184, May 2016.

[18] X. Huang, Q. Li, Q. Zhang, and J. Qin, "Power allocation for secure OFDMA systems with wireless information and power transfer," *IEEE Electronics Lett.*, vol. 50, no. 3, pp. 229–230, Jan. 2014.

[19] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 86–93, June 2015.

[20] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, Feb. 2014.

[21] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[22] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th Ed.. San Diago: Academic Press, 2000.

[23] M. S. Trotter, C. R. Valenta, G. A. Koo, B. R. Marshall, and G. D. Durgin, "Multi-antenna techniques for enabling passive RFID tags and sensors at microwave frequencies," in Prof. *IEEE International Conf. RFID*, pp. 1–7, Orlando, FL, USA, Apr. 2012.

[24] M. Gregori and M. Payaro, "Optimal power allocation for a wireless multi-antenna energy harvesting node with arbitrary input distribution," in Proc. *IEEE International Conf. on Communications*, pp. 5794–5798, Ottawa, ON, Canada, June 2012.

[25] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[26] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[27] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[28] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[29] S. Hessien, F. S. Al-Qahtani, R. M. Radaydeh, C. Zhong, and H. Alnuweiri, "On the secrecy enhancement with low-complexity large-scale transmit selection in MIMO generalized composite fading," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 429–432, Aug. 2015.

[30] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[31] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inform. Foren. Sec.*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[32] Z. Ding, S. M. Perlaza, I. Esnaola, and H. V. Poor, "Power allocation strategies in energy harvesting wireless cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 846–860, Feb. 2014.

[33] G. Zhu, C. Zhong, H. Suraweera, G. K. Karagiannids, Z. Zhang, and T. Tsiftsis, "Wireless information and power transfer in relay systems with multiple antennas and interference," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1400–1418, Apr. 2015.

[34] C. Zhong, X. Chen, Z. Zhang, and G. K. Karagiannidis, "Wireless-powered communications: Performance analysis and optimization," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5178–5190, Dec. 2015.

[35] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge, U.K.: Cambridge Univ. Press, 2005.

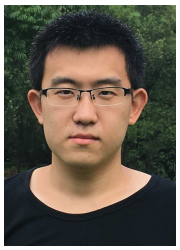
[36] A. M. Magableh and M. M. Matalgah, "Capacity of SIMO systems over non-identically independent Nakagami-m channels," in *Proc. IEEE Sarnoff Symposium*, Nassau Inn, Princeton, NJ, April 2007, pp. 1–5.

[37] M. K. Simon and M. S. Alouini, "Digital Communication over Fading Channels: A Unified Approach to Performance Analysis," Hoboken, NJ: Wiley, 2000.

[38] A. Shah and A. M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1454–1463, July 2000.

[39] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787-1791, Oct. 2010.

[40] A. P. Prudnikow, Y. A. Brychkov, and O. I. Marchev, *Integrals and Series: More Special Functions*, vol. 3, New York, NY, USA: Gordon and Breach, 1990.
[41] K. Tourki, F. A. Khan, K. A. Qaraqe, H. Yang, and M. Alouini, "Exact performance analysis of MIMO cognitive radio systems using transmit antenna selection," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 425–438, Mar. 2014.



Xin Jiang (S'16) received the B.S. degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2015. He is currently working towards his M.S. degree in the college of information science and electronic engineering at Zhejiang University. His research interests include physical layer security and wireless powered communications.

Caijun Zhong (S'07-M'10-SM'14) received the B.S. degree in Information Engineering from the Xi'an Jiaotong University, Xi'an, China, in 2004, and the M.S. degree in Information Security in 2006, Ph.D. degree in Telecommunications in 2010, both from University College London, London, United Kingdom. From September 2009 to September 2011, he was a research fellow at the Institute for Electronics, Communications and Information Technologies (ECIT), Queens University Belfast, Belfast, UK. Since September 2011, he has been with Zhejiang University, Hangzhou, China, where he is currently an associate professor. His research interests include massive MIMO systems, full-duplex communications, wireless power transfer and physical layer security.

Dr. Zhong is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, and JOURNAL OF COMMUNICATIONS AND NETWORKS. He is the recipient of the 2013 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award. He and his coauthors has been awarded a Best Paper Award at the WCSP 2013. He was an Exemplary Reviewer for IEEE TRANSACTIONS ON COMMUNICATIONS in 2014.

Xiaoming Chen (M'10-SM'14) received the B.Sc. degree from Hohai University in 2005, the M.Sc. degree from Nanjing University of Science and Technology in 2007 and the Ph. D. degree from Zhejiang University in 2011, all in electronic engineering. He is currently with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. Since Feberuary 2015, he is a Humboldt Resarch Fellow at the Institute for Digital Communications, University of Erlangen-Nürnberg, Erlangen, Germany. His research interests mainly focus on multiple-antenna techniques, wireless security, interference network and wireless power transfer, etc.

Dr. Chen serves as an Associate Editor for the IEEE ACCESS and an Editor for the IEEE COMMUNICATIONS LETTERS. He was honoured as an Exemplary Reviewer of the IEEE Communications Letters in 2014 and the IEEE Transactions on Communications in 2015.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of 190 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020).

Theodoros A. Tsiftsis (S'02, M'04, SM'10) was born in Lamia, Greece, in 1970. He received the B.Sc. degree in physics from the Aristotle University of Thessaloniki, Greece, in 1993, the M.Sc. degree in digital systems engineering from the Heriot-Watt University, Edinburgh, U.K., in 1995, the M.Sc. degree in decision sciences from the Athens University of Economics and Business, Greece, in 2000, and the Ph.D. degree in electrical engineering from the University of Patras, Greece, in 2006. He joined the Department of Electrical Engineering at the Technological Educational Institute of Central Greece in February 2010. Currently, he is Associate Professor of Communication Technologies in the Department of Electrical and Electronic Engineering at the School of Engineering of the Nazarbayev University, Astana, Kazakhstan. His research interests include the broad areas of cooperative communications, communication theory, wireless communications, and optical wireless communication systems.

Dr. Tsiftsis acts as reviewer for several international journals and he was member of the Editorial Boards of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE COMMUNICATIONS LETTERS. Currently he is an Area Editor for Wireless Communications II of the IEEE TRANSACTIONS ON COMMUNICATIONS.

Zhaoyang Zhang (M02) received his Ph.D. degree in communication and information systems from Zhejiang University, China, in 1998. He is currently a full professor with the Department of Information Science and Electronic Engineering, Zhejiang University. His research interests are mainly focused on information theory and coding theory, signal processing for communications and in networks, and their applications in the next generation wireless mobile communication systems. He has co-authored more than 150 refereed international journal and conference papers as well as two books in the above areas. He was a co-recipient of several conference Best Paper Awards / Best Student Paper Award. He is currently serving as Editor for IEEE TRANSACTIONS ON COMMUNICATIONS, IET COMMUNICATIONS and some other international journals. He has served or is serving as TPC Co-Chair or Symposium Co-Chair for many international conferences like WCSP 2013, ICUFN2011/12/13, and Globecom 2014 Wireless Communications Symposium, etc.